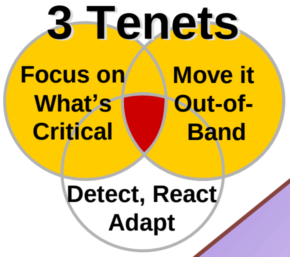
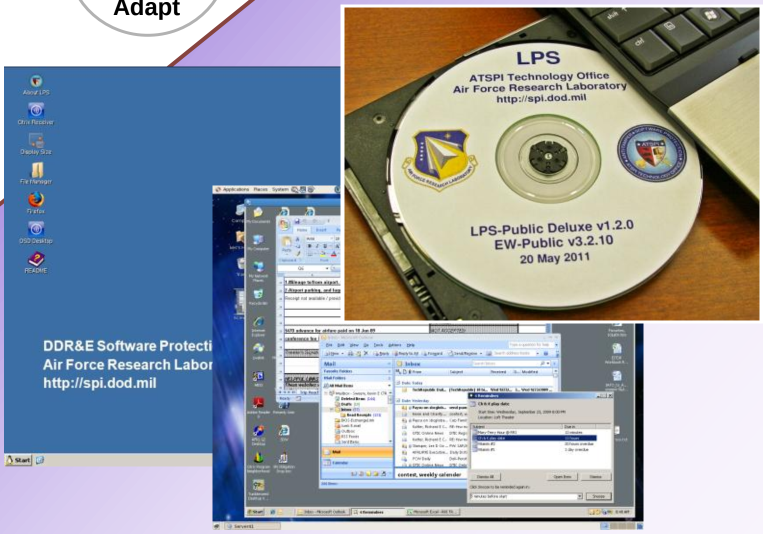


Lightweight Portable Security (LPS)

LPS-Remote Access Edition



Secure Remote Access

- Creates a trusted end-node
- Low total-cost telework solution
- Virtual Private Network (VPN) support
- CAC/PIV middleware built in
- Custom LiveCD built for your network
- Easily deployed
- Accredited

Virtual GFE Secure End-Node Technology

Booting from a CD and installing nothing, the Lightweight Portable Security (LPS) family of products creates a temporary, RAM-based, secure end-node on almost any computer. The **LPS-Remote Access** edition provides secure, low-cost, desktop virtualization via remote access. LPS-Remote Access creates a trusted “virtual GFE” (Government-Furnished Equipment) environment within minutes on almost any Intel-based computer (Mac or PC).

In 2009, LPS-Remote Access was evaluated by NSA, approved by the ASD NII (DoD CIO) for DoD-wide use during pandemic emergencies, and certified by AFNIC/EV for the AF-GIG for emergency use. It received a Certificate of Networthiness from the US Army in 2011. It is the only DoD-approved remote access solution using non-GFE. Compared to other solutions, LPS-Remote Access is faster to deploy and cheaper to maintain.

Your Custom Build

We will create a custom LPS-Remote Access build for your specific connectivity and remote desktop infrastructure. Our team will work with you to hone your build by setting specific ports, protocols, and services, and adding any optional application software. Start by visiting **https://spi.dod.mil/COOP/ DoD_form_SSL.htm**.

Deploying LPS-Remote Access

Initial deployment and support documents are provided with the customized ISO image. The files and Tier 2 support are furnished without charge to DoD units; organizations incur any costs for deployment and sustainment. SPI also offers developer tools, source code, the certification memo, and vulnerability assessments.

A High Security, Tightly Focused Solution

The ATSPI Technology Office designed LPS-Remote Access for maximum security, focusing specifically on providing temporary remote access only. LPS-Remote Access boots from a LiveCD and resides in RAM; the local disk is not touched. It intentionally lacks drivers for hard drives, printers, and most USB devices. Its firewall can be customized to allow only outbound connections to authorized addresses. The LPS-Remote Access build holds only a tightly configured Firefox browser and the remote access tools and clients you need to access your enterprise network.

LPS implements Information Assurance’s highest principles. Booting a pristine operating system assures integrity. Encrypted communication and non-persistence provide confidentiality and privacy. One’s smart card or login/password provides authenticity and non-repudiation. Using almost any computer provides availability and continuity. Finally, keeping data and tools centralized minimizes costs and exfiltration, enables full audits, and eases compliance.

LPS-Remote Access Support Organization Prerequisites

- Request, receive, and burn ISO images
- Deploy CDs, USB smart card readers, and user materials
- Network resources to support remote users
- Tier 1 support of your custom build and network

LPS-Remote Access System Requirements

- x86 PC or Mac, bootable CD-ROM drive
- 512 MB RAM minimum (1 GB for OpenOffice version)
- Wired , WiFi, or Cellular Broadband Internet connection
- CAC/PIV in CCID-compliant USB smart card reader

ATSPI Technology Office. Protecting DoD intellectual property in the cyber domain.
Learn more at **spi.dod.mil.** Contact us at **ATSPI_outreach@wpafb.af.mil.**

Approved for Public Release: 12 June 2009, 88 ABW 09-2567